PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 16 August 2000 (16.08.00)	
International application No. PCT/EP99/09844	**Applicant's or agent's file reference** P98116WO.1P
International filing date (day/month/year) 09 December 1999 (09.12.99)	**Priority date** (day/month/year) 18 January 1999 (18.01.99)
Applicant HEISTER, Ulrich	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

10 July 2000 (10.07.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Charlotte ENGER

Telephone No.: (41-22) 338.83.38

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70) 4

Applicant's or agent's file reference P98116WO.1P	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP99/09844	International filing date (*day/month/year*) 09 December 1999 (09.12.99)	Priority date (*day/month/year*) 18 January 1999 (18.01.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/20		
Applicant DEUTSCHE TELEKOM AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 2 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 July 2000 (10.07.00)	11 April 2001 (11.04.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/09844

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-6, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 4-7, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-3, filed with the letter of 15 March 2001 (15.03.2001),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/1, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-7	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-7	NO
Industrial applicability (IA)	Claims	1-7	YES
	Claims		NO

2. Citations and explanations

General observations

The position taken by the applicant in the letter of 13 March 2001 gives no reason to depart from the already communicated opinion, since the submitted amendments are not sufficient to eliminate the objections raised in the first written opinion of 12 January 2001.

The applicant has given in the letter of 13 March 2001 various explanations to clarify some vague formulations in the claims and has pointed out differences between the present application and the prior art as represented by the cited article, "ATM cell encryption and key update snychronization". In this respect, it is noted that the scope of protection to be assessed is based only on the subject matter defined by the wording of the claims and not on examples given in the description or explanations in a letter of response.

The applicant is requested to note that the clarity of the claims is of utmost importance because the preliminary examination report can be based only on the subjects defined by the wording of the claims, and not on supposed differences from the prior art contained in the

description or the figures of the application. A claim must therefore be clear *per se*, and the claimed scope of protection as well as the meaning of the individual features must be clear from the wording of the claim alone (see PCT International Preliminary Examination Guidelines, PCT Gazette, Section IV, Chapter III, 4.1-4.4).

CLAIMS 1 AND 4

The present application addresses the problem of providing a method and device for synchronising an ATM-cell stream encrypter with an ATM-cell stream decrypter which can be implemented without requiring additional capacity and with as little outlay as possible.

As far as shown by the very broad wording of Claims 1 and 4, the main feature of the proposed solution to this problem consists in associating a (logical) state automaton to the ATM-cell stream encrypter and to the ATM-cell stream decrypter and in modifying the variable encryption key, as well as the secret key, depending on the (logical) state of the state automaton.

Neither the problem addressed nor the solution indicated can be considered inventive (PCT Article 33(3)) because both the problem and the feature of the solution can already be found in an equivalent form in one of the prior art documents cited in the search report.

The article "ATM cell encryption and key update synchronization" by James Gray et al. (see, in particular, the abstract; page 402, lines 11-23; page 403, lines 6-18; page 403; Figures 5 and 6 with the corresponding text passages on pages 403-405) describes a synchronisation system in which a "marker cell" transmitted in the ATM

cell stream is used to modify the key at both ends of the ATM transmission path in a corresponding manner in order to synchronise encryption and decryption at the transmitter and receiver ends. The momentary state of the detected ATM cells is polled and taken into account for forming the key (see the indicated passages on pages 402-405).

Although said article does not explicitly list all the components indicated in Claims 1 and 4, and the known synchronisation system, unlike the system as per Claims 1 and 4, transmits a particular "marker cell" in order to inform the receiver of the moment in time when decryption should be carried out with the new key, it is clear that for that system to recognise the marker cells transmitted, it must comprise a device for recognising the cell boundaries, as well as a device for recognising the content (state) of the marker cells. Consequently, these system components can also be found, albeit implicitly, in the cited article (see the passages indicated on pages 402-405).

The subject matter of Claims 1 and 4 therefore cannot be acknowledged to involve an inventive step in relation to the cited prior art (PCT Article 33(3)).

CLAIMS 2, 3 and 5-7

Insofar as the partially unclear wording of the dependent claims is comprehensible, these claims do not contain any additional features which, in combination with each other or with the subject matter of Claims 1 or 4, involve an inventive step. The essential features of these claims are either known or can be directly derived from the cited article or from one of the search report citations (see

the already indicated text passages).

The present dependent claims therefore also fail to meet the requirements of PCT Article 33(3).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The introductory part of the description has not acknowledged the cited reference document (see Box V) as prior art (PCT Rule 5.1(a)(ii)).

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

CLAIMS 1 and 4

The expressions and formulations used in Claims 1 and 4, "stream encrypter" and "stream decrypter", "cell boundary recognition", "state automaton" and "state", are misleading and leave the reader in doubt about the meaning of the technical features in question. As a result, the definition of the subjects of Claims 1 and 4 is not clear and the requirements of PCT Article 6 are not met.

The above-mentioned formulations not only affect the clarity of Claims 1 and 4 but also raise doubts regarding the exact scope of protection. It is noted that a claim must be clear *per se* so that the meaning of the individual features is clear from the wording of the claim alone (see the PCT International Preliminary Examination Guidelines, PCT-Gazette, Chapter III, 4).

Moreover, in line 6 of Claim 1, the statement "and stream encrypter each comprise an ATM cell...", is unclear.

Consequently, Claims 1 and 4 do not meet the requirements of PCT Article 6.

CLAIMS 2 and 6

The entire wording of dependent Claim 2 is unclear and therefore its scope of protection cannot be determined.

The expressions "for forming a function" and "using a predetermined function" in Claims 2 and 6 are not clear

VIII. Certain observations on the international application

because the functions concerned have not been defined. Moreover, the description also fails to indicate what functions are concerned and therefore this measure is not sufficiently supported by the description.

Claims 2 and 6 therefore also fail to meet the requirements of PCT Article 6.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
P98116WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/09844	09/12/1999	18/01/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/20		
Anmelder DEUTSCHE TELEKOM AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 8 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 2 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
10/07/2000	11.04.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Ferrari, J Tel. Nr. +49 89 2399 8803

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/09844

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1-6	ursprüngliche Fassung				

Patentansprüche, Nr.:

4-7	ursprüngliche Fassung				
1-3	eingegangen am	15/03/2001	mit Schreiben vom	13/03/2001	

Zeichnungen, Blätter:

1/1	ursprüngliche Fassung				

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-7
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	
	Nein:	Ansprüche	1-7
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-7
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

Allgemeine Bemerkungen

Die mit Schreiben vom 13.03.2001 eingereichte Stellungnahme des Anmelders gibt keinen Anlaß von der bereits mitgeteilten Auffassung abzuweichen, da die eingereichten Änderungen nicht ausreichen, um die im ersten schriftlichen Bescheid vom 12.01.2001 erhobenen Einwände zu beheben.

Der Anmelder hat in seinem Schreiben vom 13.03.2001 verschiedene Erklärungen zur Klarstellung einiger vager Formulierungen in den Ansprüchen abgegeben, und hat Unterschiede der vorliegenden Anmeldung zum Stand der Technik gemäß dem genannten Artikel "ATM cell encryption and key update synchronization" herausgestellt. Hierzu wird darauf hingewiesen, daß der zu analysierende Schutzbereich nur auf dem Gegenstand, wie er durch den Wortlaut der Ansprüche definiert ist, basiert, und nicht aufgrund von Beispielen in der Beschreibung oder von Erklärungen in einem Antwortschreiben.

In diesem Zusammenhang wird der Anmelder darauf hingewiesen, daß die Klarheit der Ansprüche von äußerster Bedeutung ist, da der vorläufige Prüfungsbericht lediglich auf der Grundlage des Wortlautes der in den Ansprüchen definierten Gegenstände erfolgen kann, und nicht aufgrund vermeintlicher Unterschiede zum Stand der Technik die in der Beschreibung bzw. den Figuren der Anmeldung enthalten sein können. Ein Anspruch muß daher in sich klar sein, so daß sowohl der beantragte Schutzbereich als auch die Bedeutung der einzelnen Merkmale aus dem Wortlaut des Anspruchs allein deutlich werden (vgl. Richtlinien für die internationale vorläufige Prüfung, PCT-Gazette/Section IV/Kapitel III, 4.1 - 4.4).

Bemerkungen zum Absatz V.:

ANSPRÜCHE 1, 4

Der vorliegenden Anmeldung liegt die Aufgabenstellung zugrunde, ein Verfahren und eine Anordnung zur Synchronisation eines ATM-Zellenstromchiffrierers mit einem ATM-Zellenstromdechiffrierers anzugeben, welches keine zusätzliche Kapazität benötigt und mit möglichst geringem Aufwand zu implementieren ist.

Soweit aus dem sehr breit verfaßten Wortlaut der Ansprüche 1 und 4 entnehmbar, wird als Hauptmerkmal zur Lösung dieser Aufgabe vorgeschlagen, dem ATM-Zellenstromchiffrierer und dem ATM-Zellenstromdechiffrierer einen (logischen) Zustandsautomaten zuzuordnen, und den variablen Chiffrier-Schlüssel neben dem geheimen Schlüssel ebenfalls abhängig vom (logischen) Zustand des Zustandsautomaten zu ändern.

Weder die genannte Aufgabenstellung, noch die angegebene Lösung können hierbei als Erfinderisch im Sinne von Artikel 33(3) PCT angesehen werden, da sowohl das Problem als auch das Lösungsmerkmal bereits in equivalenter Weise aus einem im Recherchenbericht aufgeführten Dokument des Standes der Technik entnehmbar sind.

Aus dem Artikel "ATM cell encryption and key update synchronization" von James Gray et al. (vgl. insbes. Zusammenfassung; Seite 402, Zeilen 11-23; Seite 403, Zeilen 6-18; Seite 403, Figuren 5 und 6 mit den zugehörigen Textpassagen auf den Seiten 403-405) ist ein Synchronisationssystem bekannt, bei dem zur Synchronisation der Chiffrierung/Dechiffrierung von Sender- und Empfängerseite mit Hilfe einer im ATM-Zellenstrom gesendeten "marker cell" der Schlüssel entsprechend auf beiden Seiten der ATM-Übertragungsstrecke geändert wird. Der jeweilige Zustand der detektierten ATM-Zellen wird abgefragt und zur Bildung des Schlüssels entsprechend berücksichtigt (vgl. angegebene Passagen auf den Seiten 402-405).

Obwohl nicht alle die in den Ansprüchen 1 und 4 genannten Komponenten explizit in dem genannten Artikel aufgeführt werden, und das bekannte Synchronisationssystem, im Gegensatz zu dem System gemäß den Ansprüchen 1 und 4, eine bestimmte "marker cell" überträgt um dem Empfänger den Zeitpunkt mitzuteilen wann die Entschlüsselung mit dem neuen Schlüssel durchzuführen ist, ist es klar, daß zur Erkennung der gesendeten Marker-Zellen eine Einrichtung zur Zellgrenzerkennung sowie eine Einrichtung zur Erkennung des Inhalts (Zustand) dieser Marker-Zellen vorhanden sein müssen. Diese Systemkomponenten sind daher ebenfalls, und zwar implizit, aus dem genannten Artikel entnehmbar (vgl. angegebene Passagen auf den Seiten 402-405).

Hinsichtlich des genannten Standes der Technik kann dem Gegenstand der Ansprüche 1 und 4 somit keine erfinderische Tätigkeit im Sinne von Artikel 33(3) PCT zuerkannt werden.

ANSPRÜCHE 2, 3, 5-7

Soweit aus dem teilweise unklaren Wortlaut der abhängigen Ansprüche entnehmbar, enthalten diese keine zusätzlichen Merkmale, die in Kombination miteinander oder mit dem Gegenstand des Anspruchs 1 oder 4 eine erfinderische Tätigkeit beinhalten. Die wesentlichen Merkmale dieser Ansprüche sind entweder aus dem genannten Artikel, oder aus einem der im Recherchenbericht zitierten Dokumente, bekannt oder direkt daraus herleitbar (vgl. die bereits angegebenen Textpassagen).

Die Erfordernisse des Artikels 33(3) PCT sind daher für die vorliegenden abhängigen Ansprüche ebenfalls nicht erfüllt.

Bemerkungen zum Absatz VII.:

Die genannte Entgegenhaltung (siehe Absatz V) ist nicht als Stand der Technik in der Beschreibungseinleitung gewürdigt worden, Regel 5.1 (a)(ii) PCT.

Bemerkungen zum Absatz VIII.:

ANSPRÜCHE 1, 4

Die in den Ansprüchen 1 und 4 benutzten Ausdrücke und Formulierungen
"Stromchiffrierer" bzw. "Stromdechiffrierer";
"Zellgrenzerkennung";
"Zustandsautomat" bzw. "Zustand"
sind irreführend und unklar und lassen den Leser über die Bedeutung der betreffenden technischen Merkmale im Ungewissen. Dies hat zur Folge, daß die Definition der Gegenstände der Ansprüche 1 und 4 nicht klar ist und somit die Erfordernisse des Artikels 6 PCT nicht erfüllt sind.

Die oben genannten Formulierungen beinträchtigen nicht nur die Klarheit der Ansprüche 1 und 4, sondern lassen ebenfalls Zweifel über den genauen Schutzbereich entstehen. Hierbei wird darauf hingewiesen, daß ein Anspruch in sich klar sein muß, so daß die Bedeutung der einzelnen Merkmale aus dem Wortlaut des Anspruchs allein deutlich wird (vgl. Richtlinien für die internationale vorläufige Prüfung, PCT-Gazette, Kapitel III-4).

Ferner ist in der Zeile 6 des Anspruchs 1 der Wortlaut "...und Stromchiffrierer (..) ATM-Zelle jeweils einen ..) unklar.

Ansprüche 1 und 4 erfüllen daher nicht die Erfordernisse des Artikels 6 PCT.

ANSPRÜCHE 2, 6

Der gesamte Wortlaut des abhängigen Anspruchs 2 ist unklar, so daß dessen Schutzbereich nicht feststellbar ist.

Die Begriffe "zur Bildung einer Funktion", und "mit Hilfe einer vorgegebenen Funktion" in den Ansprüchen 2 und 6 ist nicht klar, da nicht definiert wurde um welche

Funktion es sich hierbei handelt. Außerdem geht aus der Beschreibung ebenfalls nicht hervor um welche Funktion es sich hierbei handelt, sodaß diese Maßnahme nicht ausreichend durch die Beschreibung gestützt ist.

Ansprüche 2 und 6 erfüllen daher ebenfalls nicht die Erfordernisse des Artikels 6 PCT.

Bemerkungen zum Absatz V.:

ANSPRÜCHE 1, 4

Der vorliegenden Anmeldung liegt die Aufgabenstellung zugrunde, ein Verfahren und eine Anordnung zur Synchronisation eines ATM-Zellenstromchiffrierers mit einem ATM-Zellenstromdechiffrierers anzugeben, welches keine zusätzliche Kapazität benötigt und mit möglichst geringem Aufwand zu implementieren ist.

Soweit aus dem sehr breit verfaßten Wortlaut der Ansprüche 1 und 4 entnehmbar, wird als Hauptmerkmal zur Lösung dieser Aufgabe vorgeschlagen, dem ATM-Zellenstromchiffrierer und dem ATM-Zellenstromdechiffrierer einen (logischen) Zustandsautomaten zuzuordnen, und den variablen Chiffrier-Schlüssel neben dem geheimen Schlüssel ebenfalls abhängig vom (logischen) Zustand des Zustandsautomaten zu ändern.

Weder die genannte Aufgabenstellung, noch die angegebene Lösung können hierbei als Erfinderisch im Sinne von Artikel 33(3) PCT angesehen werden, da sowohl das Problem als auch das Lösungsmerkmal bereits in equivalenter Weise aus einem im Recherchenbericht aufgeführten Dokument des Standes der Technik entnehmbar sind.

Aus dem Artikel "ATM cell encryption and key update synchronization" von James Gray et al. (vgl. insbes. Zusammenfassung; Seite 402, Zeilen 11-23; Seite 403, Zeilen 6-18; Seite 403, Figuren 5 und 6 mit den zugehörigen Textpassagen auf den Seiten 403-405) ist ein Synchronisationssystem bekannt, bei dem zur Synchronisation der Chiffrierung/Dechiffrierung von Sender- und Empfängerseite mit Hilfe einer im ATM-Zellenstrom gesendeten "marker cell" der Schlüssel entsprechend auf beiden Seiten der ATM-Übertragungsstrecke geändert wird. Der jeweilige Zustand der detektierten ATM-Zellen wird abgefragt und zur Bildung des Schlüssels entsprechend berücksichtigt (vgl. angegebene Passagen auf den Seiten 402-405).

Obwohl nicht alle die in den Ansprüchen 1 und 4 genannten Komponenten explizit in dem genannten Artikel aufgeführt werden, und das bekannte Synchronisationssystem, im Gegensatz zu dem System gemäß den Ansprüchen 1 und 4, eine bestimmte "marker cell" überträgt um dem Empfänger den Zeitpunkt mitzuteilen wann die Entschlüsselung mit dem neuen Schlüssel durchzuführen ist, ist es klar, daß zur Erkennung der gesendeten Marker-Zellen eine Einrichtung zur Zellgrenzerkennung sowie eine Einrichtung zur Erkennung des Inhalts (Zustand) dieser Marker-Zellen vorhanden sein müssen. Diese Systemkomponenten sind daher ebenfalls, und zwar implizit, aus dem genannten Artikel entnehmbar (vgl. angegebene Passagen auf den Seiten 402-405).

Hinsichtlich des genannten Standes der Technik kann dem Gegenstand der Ansprüche 1 und 4 somit keine erfinderische Tätigkeit im Sinne von Artikel 33(3) PCT zuerkannt werden.

ANSPRÜCHE 2, 3, 5-7

Soweit aus dem teilweise unklaren Wortlaut der abhängigen Ansprüche entnehmbar, enthalten diese keine zusätzlichen Merkmale, die in Kombination miteinander oder mit dem Gegenstand des Anspruchs 1 oder 4 eine erfinderische Tätigkeit beinhalten. Die wesentlichen Merkmale dieser Ansprüche sind entweder aus dem genannten Artikel, oder aus einem der im Recherchenbericht zitierten Dokumente, bekannt oder direkt daraus herleitbar (vgl. die bereits angegebenen Textpassagen).

Die Erfordernisse des Artikels 33(3) PCT sind daher für die vorliegenden abhängigen Ansprüche ebenfalls nicht erfüllt.

Bemerkungen zum Absatz VII.:

Die genannte Entgegenhaltung (siehe Absatz V) ist nicht als Stand der Technik in der Beschreibungseinleitung gewürdigt worden, Regel 5.1 (a)(ii) PCT.

Bemerkungen zum Absatz VIII.:

ANSPRÜCHE 1, 4

Die in den Ansprüchen 1 und 4 benutzten Ausdrücke und Formulierungen
"Stromchiffrierer" bzw. "Stromdechiffrierer";
"Zellgrenzerkennung";
"Zustandsautomat" bzw. "Zustand"
sind irreführend und unklar und lassen den Leser über die Bedeutung der betreffenden technischen Merkmale im Ungewissen. Dies hat zur Folge, daß die Definition der Gegenstände der Ansprüche 1 und 4 nicht klar ist und somit die Erfordernisse des Artikels 6 PCT nicht erfüllt sind.

Die oben genannten Formulierungen beinträchtigen nicht nur die Klarheit der Ansprüche 1 und 4, sondern lassen ebenfalls Zweifel über den genauen Schutzbereich entstehen. Hierbei wird darauf hingewiesen, daß ein Anspruch in sich klar sein muß, so daß die Bedeutung der einzelnen Merkmale aus dem Wortlaut des Anspruchs allein deutlich wird (vgl. Richtlinien für die internationale vorläufige Prüfung, PCT-Gazette, Kapitel III-4).

Ferner ist in der Zeile 6 des Anspruchs 1 der Wortlaut "...und Stromchiffrierer (..) ATM-Zelle jeweils einen ..) unklar.

Ansprüche 1 und 4 erfüllen daher nicht die Erfordernisse des Artikels 6 PCT.

ANSPRÜCHE 2, 6

Der gesamte Wortlaut des abhängigen Anspruchs 2 ist unklar, so daß dessen Schutzbereich nicht feststellbar ist.

Die Begriffe "zur Bildung einer Funktion", und "mit Hilfe einer vorgegebenen Funktion" in den Ansprüchen 2 und 6 ist nicht klar, da nicht definiert wurde um welche

Funktion es sich hierbei handelt. Außerdem geht aus der Beschreibung ebenfalls nicht hervor um welche Funktion es sich hierbei handelt, sodaß diese Maßnahme nicht ausreichend durch die Beschreibung gestützt ist.

Ansprüche 2 und 6 erfüllen daher ebenfalls nicht die Erfordernisse des Artikels 6 PCT.

Neue Ansprüche 1 bis 3

1. Einrichtung zur Synchronisation mindestens eines Stromdechiffrierers (7, 11; 8, 12), der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer (5, 6), wobei Stromchiffrierer (5, 6) und Stromdechiffrierer (7, 11; 8, 12) ATM-Zelle jeweils einen Pseudo-Random-Generator (6; 11; 12) aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüssel erzeugt, dadurch gekennzeichnet, daß dem Stromchiffrierer (5, 6) und dem mindestens einen Stromdechiffrierer (7, 11; 8, 12) jeweils eine Einrichtung (9; 10) zur Zellgrenzerkennung und ein Zustandsautomat (16; 17; 18) zugeordnet ist, wobei der Zustandsautomat (16; 17; 18) von der Einrichtung (9; 10) zur Zellgrenzerkennung weiterschaltbar ist und der jeweilige Zustand neben dem geheimen Schlüssel zur Bildung des variablen Schlüssels dient.

2. Einrichtung nach Anspruch 1, dadurch gekennzeichnet, daß der jeweilige Zustand des Zustandsautomaten (16; 17; 18) einer Einrichtung (19; 20; 21) zur Bildung einer vorgegebenen Funktion in Abhängigkeit vom Zustand des Zustandsautomaten (16; 17; 18) und dem geheimen Schlüssel zuführbar ist und daß die Einrichtung (19; 20; 21) zur Bildung einer vorgegebenen Funktion zur Steuerung des Pseudo-Random-Generators (6; 11; 12) ausgebildet ist.

...

3. Einrichtung nach einem der vorhergehenden Ansprüche, wobei an den Übertragungskanal mehrere Empfänger mit jeweils einem Stromdechiffrierer (7, 11; 8, 12) angeschlossen sind und wobei Kopffelder der ATM-Zellen Informationen darüber enthalten, welche Empfänger die ATM-Zellen zum Ziel haben, dadurch gekennzeichnet, daß der Stromchiffrierer (5, 6) zur Bildung des variablen Schlüssels aus dem geheimen Schlüssel des Ziels der jeweils gesendeten ATM-Zelle und aus dem jeweiligen Zustand ausgebildet ist und daß die Zustandsautomaten (16; 17; 18) des Stromchiffrierers (5, 6) und der Stromdechiffrierer (7, 11; 8, 12) unabhängig von dem Ziel der jeweiligen Zelle weiterschaltbar sind.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
P98116WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 99/09844	09/12/1999	18/01/1999
Anmelder		
DEUTSCHE TELEKOM AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

   [ ] wie vom Anmelder vorgeschlagen

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

   [X] keine der Abb.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/09844

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/20

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	GRAY J P ET AL: "ATM CELL ENCRYPTION AND KEY UPDATE SYNCHRONIZATION" TELECOMMUNICATION SYSTEMS,CH,BASEL, Bd. 7, Nr. 4, 1997, Seiten 391-408, XP000865923 ISSN: 1018-4864	1,2,4
A	Zusammenfassung Seite 393, Zeile 43 -Seite 394, Zeile 23 Seite 402, Zeile 11 - Zeile 36 Seite 404, Zeile 3 -Seite 405, Zeile 11 Seite 406, Zeile 1 - Zeile 16 Abbildungen 5,6	3,5-7

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem Internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem Internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche	Absendedatum des Internationalen Recherchenberichts
18. April 2000	27/04/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 673 133 A (NEDERLAND PTT) 20. September 1995 (1995-09-20) Zusammenfassung Spalte 1, Zeile 27 -Spalte 2, Zeile 9 Spalte 3, Zeile 4 - Zeile 16 Anspruch 1 Abbildung 1	1-7

INTERNATIONAL SEARCH REPORT

[illegible]ation on patent family members

[illegible]national Application No
PCT/EP 99/09844

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0673133 A	20-09-1995	NL 9400428 A	01-11-1995
		CA 2144831 A,C	19-09-1995
		US 5809147 A	15-09-1998

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/09844

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GRAY J P ET AL: "ATM CELL ENCRYPTION AND KEY UPDATE SYNCHRONIZATION" TELECOMMUNICATION SYSTEMS,CH,BASEL, vol. 7, no. 4, 1997, pages 391-408, XP000865923 ISSN: 1018-4864	1,2,4
A	abstract page 393, line 43 -page 394, line 23 page 402, line 11 - line 36 page 404, line 3 -page 405, line 11 page 406, line 1 - line 16 figures 5,6	3,5-7

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 April 2000	27/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 673 133 A (NEDERLAND PTT) 20 September 1995 (1995-09-20) abstract column 1, line 27 -column 2, line 9 column 3, line 4 - line 16 claim 1 figure 1	1-7

1

INTERNATIONALER [redacted]CHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

In[redacted]nales Aktenzeichen
PCT/EP 99/09844

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0673133 A	20-09-1995	NL 9400428 A	01-11-1995
		CA 2144831 A,C	19-09-1995
		US 5809147 A	15-09-1998

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

GORNOTT, Dietmar
Zilleweg 29
D-64291 Darmstadt
ALLEMAGNE

EINGEGANGEN
RECEIVED
14. APR. 2001
PATENTANWALT
GORNOTT

PCT

MITTEILUNG ÜBER DIE ÜBERSENDUNG DES INTERNATIONALEN VORLÄUFIGEN PRÜFUNGSBERICHTS

(Regel 71.1 PCT)

Absendedatum *(Tag/Monat/Jahr)*	11.04.2001
Aktenzeichen des Anmelders oder Anwalts: P98116WO.1P	**WICHTIGE MITTEILUNG**

Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP99/09844	09/12/1999	18/01/1999

Anmelder: DEUTSCHE TELEKOM AG et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.

2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.

3. Auf Wunsch eines ausgewählten Amts wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. **ERINNERUNG**

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Ahrens, R Tel. +49 89 2399-8136

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
P98116WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/09844	09/12/1999	18/01/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/20		
Anmelder DEUTSCHE TELEKOM AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 8 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 2 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
10/07/2000	11.04.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0. Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Ferrari, J Tel. Nr. +49 89 2399 8803

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/09844

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):

Beschreibung, Seiten:

1-6	ursprüngliche Fassung				

Patentansprüche, Nr.:

4-7	ursprüngliche Fassung				
1-3	eingegangen am	15/03/2001	mit Schreiben vom	13/03/2001	

Zeichnungen, Blätter:

1/1	ursprüngliche Fassung				

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   - ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   - ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   - ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   - ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   - ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☐ Ansprüche, Nr.:

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-7
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	
	Nein:	Ansprüche	1-7
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-7
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

Allgemeine Bemerkungen

Die mit Schreiben vom 13.03.2001 eingereichte Stellungnahme des Anmelders gibt keinen Anlaß von der bereits mitgeteilten Auffassung abzuweichen, da die eingereichten Änderungen nicht ausreichen, um die im ersten schriftlichen Bescheid vom 12.01.2001 erhobenen Einwände zu beheben.

Der Anmelder hat in seinem Schreiben vom 13.03.2001 verschiedene Erklärungen zur Klarstellung einiger vager Formulierungen in den Ansprüchen abgegeben, und hat Unterschiede der vorliegenden Anmeldung zum Stand der Technik gemäß dem genannten Artikel "ATM cell encryption and key update synchronization" herausgestellt. Hierzu wird darauf hingewiesen, daß der zu analysierende Schutzbereich nur auf dem Gegenstand, wie er durch den Wortlaut der Ansprüche definiert ist, basiert, und nicht aufgrund von Beispielen in der Beschreibung oder von Erklärungen in einem Antwortschreiben.

In diesem Zusammenhang wird der Anmelder darauf hingewiesen, daß die Klarheit der Ansprüche von äußerster Bedeutung ist, da der vorläufige Prüfungsbericht lediglich auf der Grundlage des Wortlautes der in den Ansprüchen definierten Gegenstände erfolgen kann, und nicht aufgrund vermeintlicher Unterschiede zum Stand der Technik die in der Beschreibung bzw. den Figuren der Anmeldung enthalten sein können. Ein Anspruch muß daher in sich klar sein, so daß sowohl der beantragte Schutzbereich als auch die Bedeutung der einzelnen Merkmale aus dem Wortlaut des Anspruchs allein deutlich werden (vgl. Richtlinien für die internationale vorläufige Prüfung, PCT-Gazette/Section IV/Kapitel III, 4.1 - 4.4).

PCT WELTORGANISATION FÜR GEISTIGES EIGE
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 :		(11) Internationale Veröffentlichungsnummer: WO 00/42732
H04L 9/20	A1	(43) Internationales Veröffentlichungsdatum: 20. Juli 2000 (20.07.00)

(21) Internationales Aktenzeichen: PCT/EP99/09844

(22) Internationales Anmeldedatum: 9. Dezember 1999 (09.12.99)

(30) Prioritätsdaten:
199 01 666.6 18. Januar 1999 (18.01.99) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HEISTER, Ulrich [DE/DE]; Waldstrasse 63a, D–64807 Dieburg (DE).

(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Rechtsabteilung (Patente) PA1, D–64307 Darmstadt (DE).

(81) Bestimmungsstaaten: CA, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: DEVICE AND METHOD FOR SYNCHRONISING VOLTAGE CIPHERING MACHINE IN ATM NETWORKS

(54) Bezeichnung: EINRICHTUNG UND VERFAHREN ZUR SYNCHRONISATION VON STROMCHIFFRIERERN IN ATM–NETZEN

(57) Abstract

The invention relates to a device and a method for synchronising at least one voltage deciphering machine which on the receiver side is connected to a transmission channel for ATM cells. A voltage ciphering machine is mounted in the transmission channel at transmitter level. The voltage ciphering machine and the voltage deciphering machine are both provided with a pseudo–random generator which produces a variable key which is identical at transmitter and receiver level with the aid of a secret key. A device for cell boundary detection and a state automaton are respectively associated with the voltage ciphering machine and the at least one voltage deciphering machine. The state automaton can be switched from the device for cell boundary detection and the respective state can be used along with the secret key in order to produce a variable key.

(57) Zusammenfassung

Bei einer Einrichtung und einem Verfahren zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM–Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo–Random–Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender– und empfängerseitig gleichen Schlüssel erzeugt, ist dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer jeweils eine Einrichtung zur Zellgrenzerkennung und ein Zustandsautomat zugeordnet, wobei der Zustandsautomat von der Einrichtung zur Zellgrenzerkennung weiterschaltbar ist und der jeweilige Zustand neben dem geheimen Schlüssel zur Bildung des variablen Schlüssels dient.

Einrichtung und Verfahren zur Synchronisation von Stromchiffrierern in ATM-Netzen

Beschreibung

Die Erfindung betrifft eine Einrichtung und ein Verfahren zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo-Random-Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüsselstrom erzeugt.

Im Breitband-ISDN erfolgt die Übertragung im asynchronen Transfer-Modus (ATM), wobei die Informationen in Pakete gleicher Länge verpackt sind, sogenannte ATM-Zellen, im folgenden auch Zellen genannt. Eine Zelle besteht aus einem fünf Oktett großen Kopffeld (Header) und einem 48 Oktett großen Informationsfeld, das die Nutzlast (Payload) beinhaltet. Der Kopf der Zelle dient hauptsächlich zur Kennzeichnung der Verbindung, zu der diese Zelle gehört. Diese Kennzeichnung wird als Virtual Path Identifier (VPI) und Virtual Channel Identifier (VCI) bezeichnet. Diese und andere Informationen belegen im Kopffeld insgesamt 32 Bit und werden durch einen Acht-Bit-Fehlerkorrekturcode geschützt.

Dieser Fehlerkorrekturcode - auch HEC (Header Error Control) genannt - kann bis zu Drei-Bit-Fehler erkennen und Ein-Bit-Fehler und benachbarte Doppelfehler korrigieren. Außer zum Fehlerschutz wird der HEC auch zur Zellgrenzerkennung genutzt, was unter anderem in Sigmund:

"ATM - Die Technik des Breitband-ISDN", R.v. Decker Verlag, 2. Auflage 1994.

Ein gültiges Kopffeld wird gefunden, wenn sich die aus diesen 32 Bit berechnete Prüfsequenz mit der im HEC-Feld übertragenen Prüfsequenz deckt. Die empfängerseitige Synchronisation rastet dann ein. Nach 53 Oktett wird wieder ein gültiges Kopffeld erwartet. Um den Prozeß der Zellgrenzerkennung nicht zu unterbrechen und somit die ATM-Zellsynchronisation zu erhalten, ist ein kontinuierlicher Zellenstrom erforderlich. Die ATM-Zellgrenzerkennung ist ein sehr robustes Synchronisations-Verfahren.

Bei Stromchiffrierern und Stromdechiffrierern wird eine von einem kryptographisch starken Pseudo-Random-Generator (PRG) erzeugte Pseudo-Zufallssequenz als variabler Schlüssel verwendet. Den unverschlüsselten Daten p(t) wird der variable Schlüssel k(t) modulo 2 aufaddiert. Das Ergebnis ergibt dann die verschlüsselten Daten c(t). Mit dem gleichen variablen Schlüssel k(t) erfolgt dann wiederum die Entschlüsselung. Damit jeweils der gleiche variable Schlüssel erzeugt wird, ist eine Synchronisation beider Pseudo-Random-Gneratoren erforderlich.

Die Anwendung von Stromchiffrierern und Stromdechiffrierern in einem ATM-Netz und deren Synchronisation ist durch Heister U., Killat U.: "Private and Authentic Communication in Passive Optical Networks", International Journal of Network Management, Volume 5, Number 2, March-April 1995 beschrieben. Dabei wir zur Synchronisation des Stromdechiffrierers die Übertragung eines Initialisierungs-Vektors vorgeschlagen. Dies erfordert jedoch zusätzliche Übertragungskapazität.

Aufgabe der Erfindung ist es, ein zuverlässiges Verfahren zur Synchronisation von Stromdechiffrierern anzugeben, das keine zusätzliche Kapazität benötigt und mit möglichst geringem Aufwand zu implementieren ist.

Diese Aufgabe wird bei der erfindungsgemäßen Einrichtung dadurch gelöst, daß dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer jeweils ein Zustandsautomat zugeordnet ist, der von ATM-Zelle zu ATM-Zelle weiterschaltbar ist und wobei der jeweilige Zustand neben dem geheimen Schlüssel zur Bildung des variablen Schlüssels dient.

Bei einer bevorzugten Ausführungsbeispiel kann dabei vorgesehen sein, daß der Zustand einer Einrichtunç zur Bildung einer Funktion in Abhängigkeit vom Zustand und dem geheimen Schlüssel zuführbar ist, die zur Steuerung des Pseudo-Random-Generators ausgebildet ist.

Die erfindungsgemäße Einrichtung kann sowohl zwischen optischen Leitungsanschlüssen (OLT = Optical Line Termination) als auch bei optischen Netzabschlüssen (ONT = Optical Network Termination) angewendet werden, wobei jeweils ein OLT und ein ONT über einen Pseudo-Random-Gnerator und einen Zustandsautomaten verfügen. Die Zustandsautomaten werden bei der Initialisierung des Systems alle in den gleichen Anfangszustand gesetzt. Jeder ONT hat einen geheimen Schlüssel.

Die erfindungsgemäße Einrichtung kann an sich auch bereits bei einer Übertragung zwischen einem Sender und einem Empfänger angewendet werden. Besonders vorteilhaft ist jedoch eine Weiterbildung, die darin besteht, daß beim Stromchiffrierer zur Bildung des variablen Schlüssels der

geheime Schlüssel des Ziels der jeweils gesendeten ATM-Zelle und der jeweilige Zustand dient und die Zustandsautomaten des Stromchiffrierers und der Stromdechiffrierer unabhängig von dem Ziel der jeweiligen ATM-Zelle weiterschaltbar sind. Hierbei hat jeder ONT (Optical Network Termination) einen geheimen Schlüssel, der OLT (Optical Line Termination) die geheimen Schlüssel aller ONTs.

Bei dem erfindungsgemäßen Verfahren wird die Aufgabe dadurch gelöst, daß der variable Schlüssel ferner vom Zustand eines dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer zugeordneten Zustandsautomaten abhängt, der von ATM-Zelle zu ATM-Zelle weitergeschaltet wird. Dabei ist vorzugsweise vorgesehen, daß die Weiterschaltung des Zustandsautomaten bei Erkennen einer Zellgrenze durch Vergleich einer aus dem Kopffeld berechneten Prüfsequenz mit einer ebenfalls im Kopffeld der Zelle übertragenen Prüfsequenz abgeleitet wird. Dies bedeutet keinen Mehraufwand, da Einrichtungen zur Zellgrenzerkennung in den Empfängern ohnehin benötigt werden.

Eine vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens besteht darin, daß aus dem geheimen Schlüssel und dem jeweiligen Zustand mit Hilfe einer vorgegebenen Funktion eine Eingangsgröße für den jeweiligen Pseudo-Random-Generator gebildet wird.

Besonders vorteilhaft ist das erfindungsgemäße Verfahren, wenn an den Übertragungskanal mehrere Empfänger mit jeweils einem Stromdechiffrierer angeschlossen sind und wobei Kopffelder der ATM-Zellen Informationen darüber enthalten, welche Empfänger die ATM-Zellen zum Ziel haben, dadurch, daß der Bildung des variablen Schlüssels im Stromchiffrierer der

geheime Schlüssel des Stromdechiffrierers am jeweiligen Ziel zugrundegelegt wird und daß die dem Stromchiffrierer und den Stromdechiffrierern zugeordneten Zustandsautomaten bei jeder übertragenen ATM-Zelle weitergeschaltet werden.

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 einen Ausschnitt aus einem ATM-Netz mit einem Sender und zwei Empfängern und

Fig. 2 eine schematische Darstellung eines an sich bekannten Verfahrens zur Zellgrenzerkennung.

In Fig. 1 sendet ein Sender 1, der Teil eines ansonsten nicht näher dargestellten OLT ist, einen Strom von ATM-Zellen über ein optisches Netzwerk 2 an Empfänger in ONTs, von denen lediglich zwei Empfänger 3, 4 dargestellt sind. Vor der Übertragung werden die Nutzdaten einer jeden Zelle mit einem Stromchiffrierer verschlüsselt, der aus einer Exklusiv-Oder-Schaltung 5 und einem Pseudo-Random-Generator 6 besteht, welcher der Exklusiv-Oder-Schaltung 5 jeweils einen variablen Schlüssel k1(t), k2(t) zuführt, so daß die Nutzdaten p(t) als verschlüsselte Daten c(t) zum optischen Netzwerk 2 geleitet werden. Zum Entschlüsseln sind den Empfängern 3 und 4 Stromdechiffrierer 7, 11; 8, 12 vorgeschaltet, zu welchen der Zellstrom jeweils über eine Einrichtung 9, 10 zur Erkennung der Zellgrenzen geführt wird und in denen je ein Pseudo-Random-Generator 11, 12 einen variablen Schlüssel k1(t), k2(t) ableitet, der je einer Exklusiv-Oder-Schaltung zugeleitet wird. Das von den Einrichtungen 9, 10 abgeleitete Signal zeigt die Grenze einer

Zelle an und wird auch in den Empfängern 3, 4 zur Auswertung des Kopffeldes benötigt.

Eine Einrichtung zur Zellgrenzerkennung ist in Fig. 2 schematisch dargestellt, wobei aus dem über 2 zugeführten Zellstrom jeweils 40 Bit abgegriffen werden (in der Figur steht ein Pfeil für 4 Bit). Über die Bits 9 bis 40 wird bei 13 in gleicher Weise wie beim Sender ein HEC gebildet, der in einem 8-Bit-Vergleicher 14 mit den vorangegangenen Bits 1 bis 8 verglichen wird. Bei Gleichheit wird bei 15 ein Signal abgegeben, das das Erkennen eines gültigen Kopffeldes bedeutet.

Dem Stromchiffrierer und den Stromdechiffrierern ist jeweils ein Zustandsautomat 16, 17, 18 zugeordnet, der zu Beginn jeder Zelle weitergeschaltet wird. Der dann jeweils eingenommene Zustand wird jeweils einer Einrichtung 19, 20, 21 zur Berechnung von Funktionswerten aus dem Zustand und einem geheimen Schlüssel zugeführt. Die Einrichtung 19 wird von dem Sender 1 derart gesteuert, daß je nach Ziel der Zelle ein geheimer Schlüssel k1 oder k2 angewendet wird. Die empfängerseitigen Einrichtungen 20 und 21 sind jeweils nur mit einem geheimen Schlüssel k1 bzw. k2 beaufschlagt.

Durch die Verschlüsselung mit dem Schlüssel des jeweiligen Empfängers und die Weiterschaltung der Zustandsautomaten 16, 17, 18 bei der Übertragung jeder Zelle wird an dem jeweiligen Empfänger immer der richtige variable Schlüssel k1(t) bzw. k2(t) angewendet. Die zur Synchronisation benutzte ATM-Zellgrenzerkennung ist ein sehr robustes Synchronisationsverfahren, das durch die Erfindung eine zuverlässige Dechriffrierung der übertragenen Daten ermöglicht.

Patentansprüche

1. Einrichtung zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo-Random-Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüssel erzeugt, **dadurch gekennzeichnet,**
daß dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer jeweils eine Einrichtung zur Zellgrenzerkennung und ein Zustandsautomat zugeordnet ist, wobei der Zustandsautomat von der Einrichtung zur Zellgrenzerkennung weiterschaltbar ist und der jeweilige Zustand neben dem geheimen Schlüssel zur Bildung des variablen Schlüssels dient.

2. Einrichtung nach Anspruch 1, **dadurch gekennzeichnet,**
daß der Zustand einer Einrichtung zur Bildung einer Funktion in Abhängigkeit vom Zustand und dem geheimen Schlüssel zuführbar ist, die zur Steuerung des Pseudo-Random-Generators ausgebildet ist.

3. Einrichtung nach einem der vorhergehenden Ansprüche, wobei an den Übertragungskanal mehrere Empfänger mit jeweils einem Stromdechiffrierer angeschlossen sind und wobei Kopffelder der ATM-Zellen Informationen darüber enthalten, welche Empfänger die ATM-Zellen zum Ziel haben, **dadurch gekennzeichnet,**
daß beim Stromchiffrierer zur Bildung des variablen Schlüssels der geheime Schlüssel des Ziels der jeweils gesendeten ATM-Zelle und der jeweilige Zustand dient und

die Zustandsautomaten des Stromchiffrierers und der Stromdechiffrierer unabhängig von dem Ziel der jeweiligen Zelle weiterschaltbar sind.

4. Verfahren zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo-Random-Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüssel erzeugt, **dadurch gekennzeichnet,**
daß der variable Schlüssel ferner vom Zustand eines dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer zugeordneten Zustandsautomaten abhängt, der von ATM-Zelle zu ATM-Zelle weitergeschaltet wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Weiterschaltung des Zustandsautomaten bei Erkennen einer Zellgrenze durch Vergleich einer aus dem Kopffeld berechneten Prüfsequenz mit einer ebenfalls im Kopffeld der Zelle übertragenen Prüfsequenz abgeleitet wird.

6. Verfahren nach einem der Ansprüche 4 oder 5,
dadurch gekennzeichnet,
daß aus dem geheimen Schlüssel und dem jeweiligen Zustand mit Hilfe einer vorgegebenen Funktion eine Eingangsgröße für den jeweiligen Pseudo-Random-Generator gebildet wird.

7. Verfahren nach einem der Ansprüche 4 bis 6, wobei an den Übertragungskanal mehrere Empfänger mit jeweils einem Stromdechiffrierer angeschlossen sind und wobei Kopffelder

der ATM-Zellen Informationen darüber enthalten, welche Empfänger die ATM-Zellen zum Ziel haben,
dadurch gekennzeichnet,
daß der Bildung des variablen Schlüssels im Stromchiffrierer der geheime Schlüssel des Stromdechiffrierers am jeweiligen Ziel zugrundegelegt wird und daß die dem Stromchiffrierer und den Stromdechiffrierern zugeordneten Zustandsautomaten bei jeder übertragenen ATM-Zelle weitergeschaltet werden.

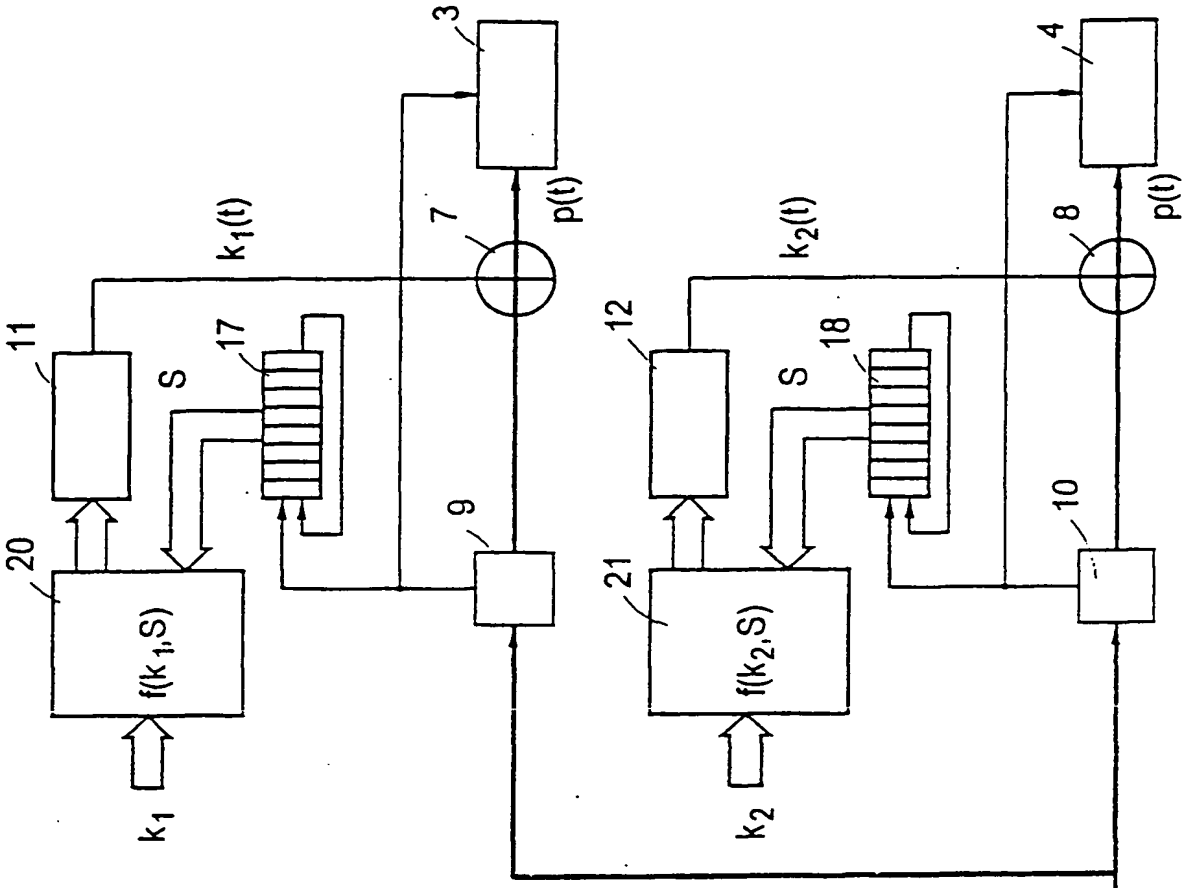
3
4
$k_1(t)$
$k_2(t)$
p(t)
7
8
11
12
17
18
S
9
10
20
21
$f(k_1,S)$
$f(k_2,S)$
k_1
k_2

Fig.1

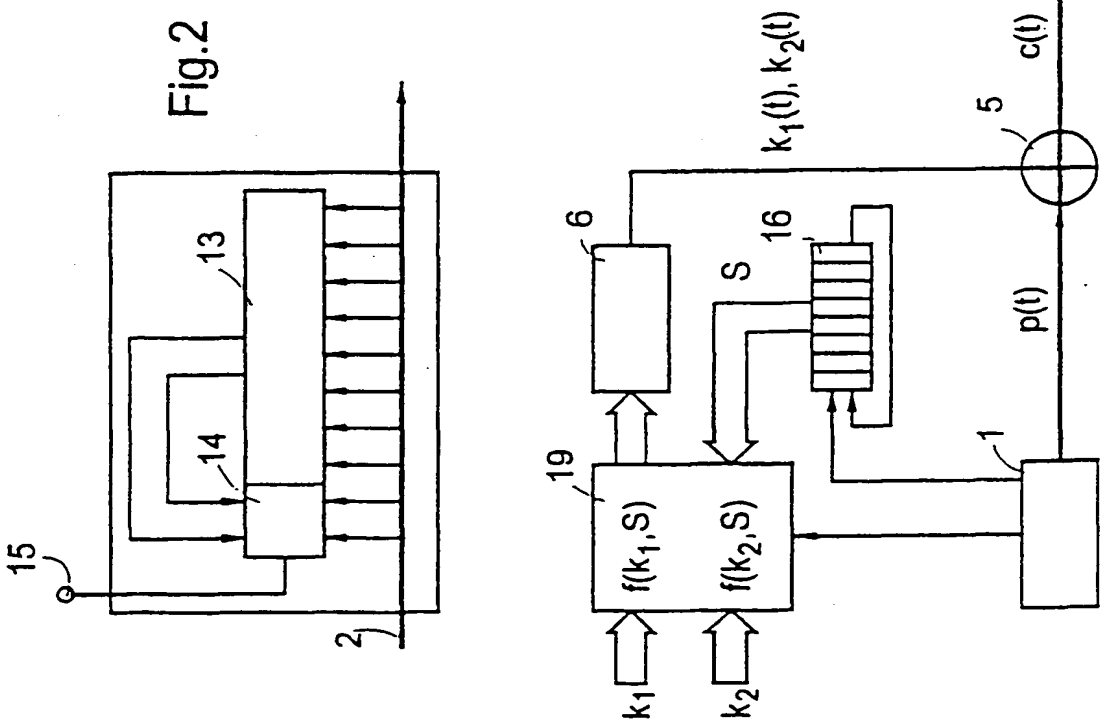
2
c(t)
$k_1(t), k_2(t)$
5
6
16
S
p(t)
19
1
$f(k_1,S)$
$f(k_2,S)$
k_1
k_2

Fig.2

13
14
15
2